REMARKS

Requirements for Information

A copy of the TEDIS Report, "Security in Open Environments" is already on file via an IDS dated May 9, 2006 and was considered by the Examiner on 6/13/06; see enclosed Form PTO/513/08a. We should emphasize that this is not prior art. In this connection, the Examiner is requested to consider the following:

1. The Examiner refers to "Mandate-final report" as "prior art". This is respectfully contested. The applicant has never admitted that this is prior art and the report was only submitted to the USPTO in response to the Examiner's earlier Requirements for Information.

2. The TEDIS Report "Security in Open Environments" was part of the PCT application as filed (from which this US application is derived); we have previously supplied evidence of this.

3. The inventor of the present invention, Professor Peter Landrock, is the author of the TEDIS Report. We have previously provided a Declaration in evidence of this.

4. We have also provided evidence in the form of the Declaration by Professor Landrock that the TEDIS Report was a confidential document, not prior art.

Claim Rejections

Claims 60-66 are in the application.

Claim 60 has been amended to meet the Examiner's objections under 35 USC 112, in particular to set forth a sequence of method steps, as requested. A number of limitations have also been added to claim 60, in particular, providing tamper-resistant document carrier hardware.

Claim 61 has been amended for consistency with amended claim 60 and to correct the lack of antecedent basis. These claims now satisfy 35 USC 112.

New dependent method claims 62 to 65 have been added and a new independent claim, claim 66, has been added directed to tamper-resistant document carrier hardware configured for splitting an END.

We request reconsideration of the rejection of claims 60 and 61 as being anticipated by Okamoto et al '162. The Examiner refers in particular to the Abstract and Background and Summary of the Invention sections of that patent.

Broadly speaking, the technique described by Okamoto employs a blind signature. The Background of the Invention outlines a number of criteria for an ideal electronic cash system (spanning pat. cols. 1 and 2) and describes an earlier system by the same inventors (spanning cols. 2 and 3) which uses a challenge-response technique to obtain information from which the user's identity can be obtained (col. 3, line 1), hence providing security. The inventors note disadvantages with their earlier system (a difficult calculation, and substantial storage requirements) and go on under Summary of the Invention to describe their new techniques which avoid the difficult calculation by using a product of two prime numbers.

For security, the system described by Okamoto et al relies upon the ability to identify the user - see, for example, pat. col. 4 lines 24 to 28:

> "that is, it is possible to utilize the principle that if the user uses electronic cash, his identity (ID), which is his secret information, is revealed through the factorization of the modulus into prime factors".

There are circumstances in which this is not sufficient.

The system described by Okamoto et al also suffers from another serious practical disadvantage, namely that once the electronic cash has been used at a store, the store must settle an account with the bank.

The Okamoto et al patent addresses the situation where a bank generates its own electronic cash "electronic cash, signed by the bank", which can only be cleared with that very bank. In other words, it is not negotiable at all. However this is a problem for electronic cash. The owner of the cash can pay the shop, and the shop can clear this with the bank that issued the cash, but the shop owner cannot go to another shop and spend the cash again.

Thus, a fundamental principle of the presently claimed invention is missing. The electronic cash cannot be negotiated twice. See, for example, pat. col. 5, lines 28 to 32:

> "the user uses the electronic cash many times to pay at various stores until the face value of his electronic cash is reached. Finally, each store settles an account with the bank **100** for each payment of electronic cash by the user".

That is, the user can spend his electronic cash at various stores but each store must then settle an account with the bank.

In complete constrast to that, the presently claimed invention specifically refers to: "transferring said END from said seller... to said buyer... splitting said END electronically... into two or more ENDs [of equal total value];...and negotiating said new ENDs separately to one or more further buyers without the involvement of a trusted third party...". This is achieved through the use of tamper-resistant document carrier hardware.

Further, Applicant's tamper-resistant document carrier hardware has a special secret key which is not accessible even to the owner of the document carrier. This is also recited in amended claim 60, to wit:

> "providing said seller with seller tamper-resistant document carrier hardware, said document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said seller" (clause 1);
>
> "providing said buyer with buyer tamper-resistant document carrier hardware, said document carrier hardware having its own public-secret key pair, and wherein said secret key is not accessible to said buyer" (clause 2).

This claimed solution to the problem is not disclosed or even hinted at in Okamoto et al. Any practical difficulties associated with the technique taught by Okamoto and et al, such as the aforementioned "... each store settles an account with the bank **100** for each payment of electronic cash by the user" has not even been recognized by them; that is, an arrangement in which each store settles an account with the bank is put forward as a positive, beneficial aspect of their invention rather than a hindrance which can prevent useful realization of the technique in practice.

Claims 61-65, being dependent on claim 60, should be allowed for the same reasons. They are allowable also in specifying additional method steps not taught by the cited reference.

Similar arguments apply, *mutatis mutandis*, in respect of new independent claim 66. Therefore, that claim should be allowed as well.

Favourable reconsideration of the application is therefore requested.

Please charge any additional fee occasioned by this paper to our Deposit Account No. 03-1237.

Respectfully submitted,

John F. McKenna
Reg. No. 20,912
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500